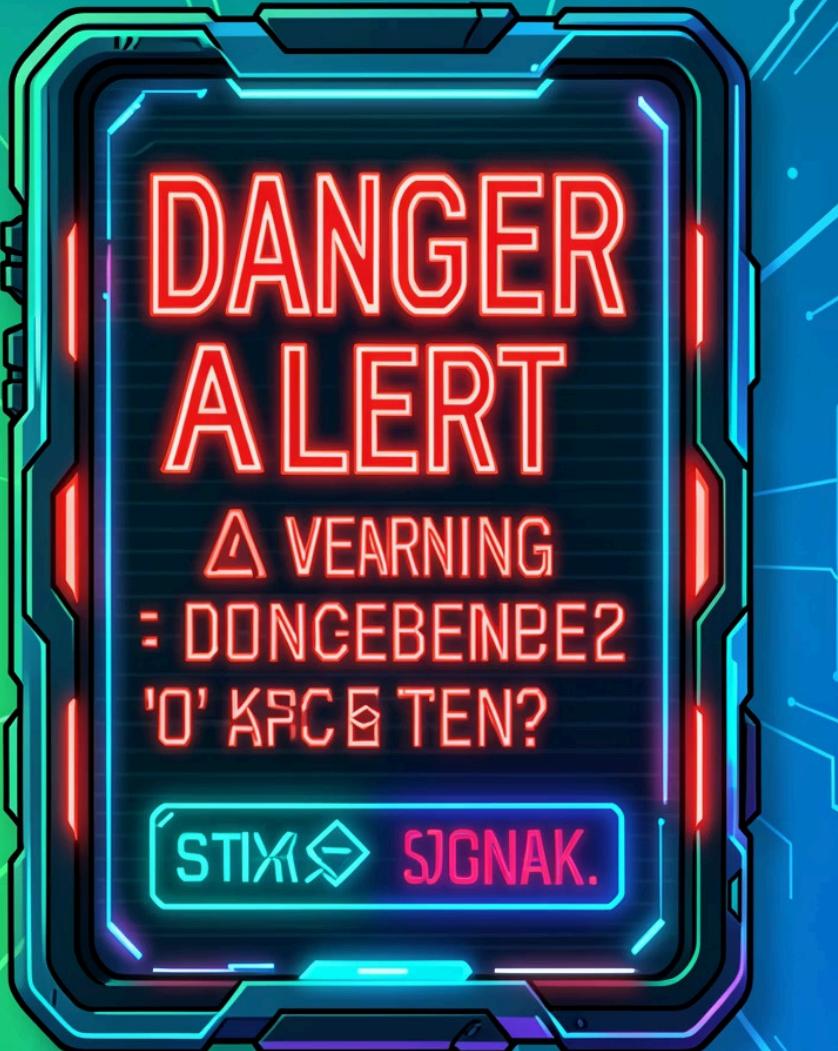


LPMA: Linux Package Manager & Auditor

Otonom Güvenlik Taraması ve Sistem Onarım Simülasyonu

AHMET ARDA SEZER

SİSTEM PROGRAMLAMA | 2026



Kritik Güvenlik Tehditleri

Paket Kaos Durumu

Linux sunucularda yüzlerce paket aktif durumda. Manuel takip ve kontrol mekanizması pratikte uygulanamaz hale gelmiştir.

CVE Zafiyetleri

Tespit edilemeyen güvenlik açıkları (CVE) sistemleri ciddi saldırı vektörlerine maruz bırakır. Zero-day açıkları kritik risk oluşturur.

Operasyonel Riskler

İnsan faktörü ve zaman kısıtları operasyonel güvenliği tehdit eder. Geciken yamalar sistem bütünlüğünü bozar.

ÇÖZÜM

LPMA: Otonom Güvenlik Katmanı

Akıllı Tarama Motoru

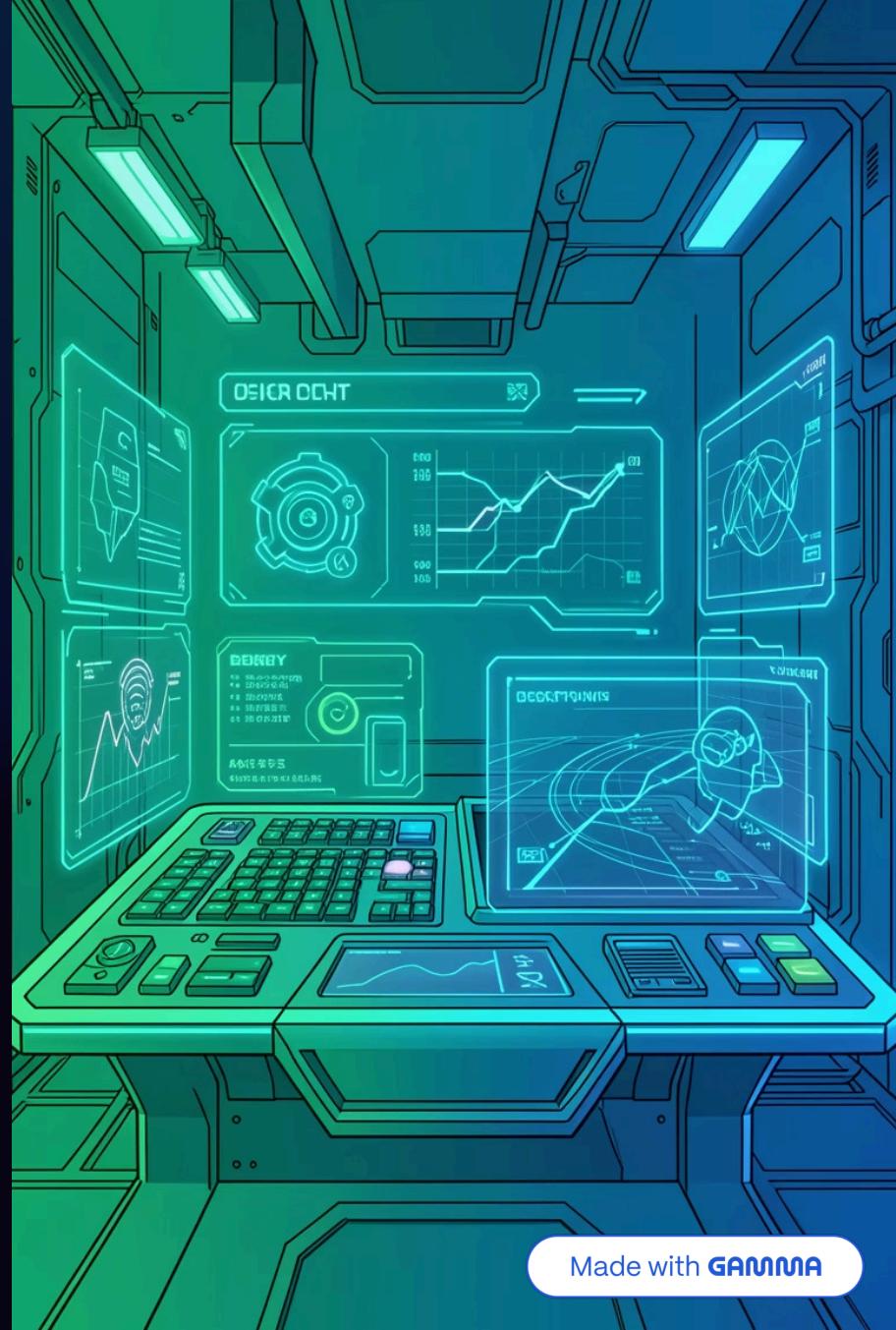
Sistemdeki tüm paketler yerel CVE veritabanı ile real-time karşılaştırılır. Zafiyet tespiti milisaniyeler içinde gerçekleşir.

Risk Sınıflandırması

Paketler **CRITICAL**, **WARN** veya **SAFE** olarak anında etiketlenir. Önceliklendirme otomatik yapılır.

Auto-Fix Mekanizması

Tek komutla zafiyetli paketler onarılır ve güncellenir. Sistem müdahalesi minimize edilir.



Teknik Altyapı ve Mimari

→ Core Logic Layer

Python tabanlı simülasyon motoru ve karar mekanizması. Zafiyet analizi ve risk hesaplama algoritmaları core'da işlenir.

→ Otomasyon Script

Bash Script (run.sh) ile native Linux entegrasyonu sağlanır. System-level operasyonlar güvenli şekilde yürütülür.

→ Audit Trail System

JSON formatında detaylı loglama. Her işlem izlenebilir, denetlenebilir formatta kaydedilir.

→ Cross-Platform

Linux ve Windows sistemlerde çalışma desteği. Platform-agnostic tasarım prensibi uygulanmıştır.

Sistem Akış Diyagramı

01

Package Enumeration

Sistem paketleri listelenip hafızaya alınır

02

CVE Database Query

Yerel veritabanı ile cross-reference yapılır

03

Vulnerability Analysis

Risk skorlaması ve sınıflandırma gerçekleşir

04

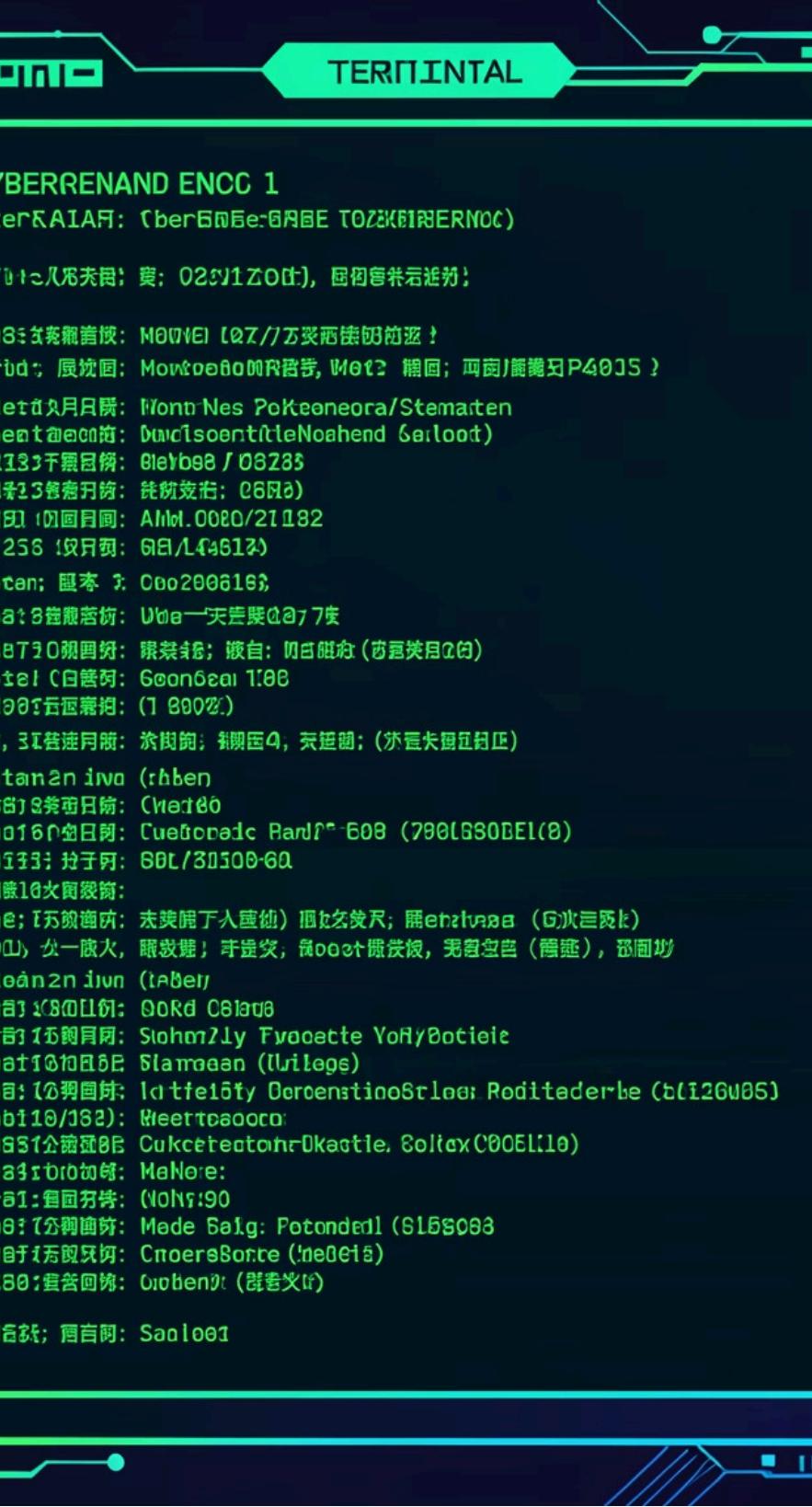
Auto-Remediation

Patch işlemleri otomatik yürütülür

05

Logging & Reporting

Tüm işlemler JSON formatında loglanır



AUDIT TRAIL

install_history.log: Şeffaflık ve İzlenebilirlik

Tam İşlem Kaydı

Sistemde yapılan her işlem `install_history.log` dosyasına otomatik yazılır. Hiçbir operasyon kayıt dışı kalmaz.

Timestamp Precision

Hangi paketin ne zaman güncellendiği saniyesi saniyesine tutulur. Forensic analiz için kritik veri sağlanır.

Version Tracking

Eski sürüm(Old Version) → Yeni Sürüm(New Version) geçişinin detaylı raporlanması. Rollback senaryoları için referans oluşturulur.

Örnek Log Çıktısı

```
{  
  "timestamp": "2026-01-15T14:23:47Z",  
  "package": "openssl",  
  "old_version": "1.1.1k",  
  "new_version": "1.1.1w",  
  "cve_fixed": ["CVE-2023-0286", "CVE-2023-0464"],  
  "severity": "CRITICAL",  
  "status": "patched",  
  "execution_time": "2.34s"  
}
```

JSON Format

Makine-okunabilir format SecOps araçlarına entegrasyon sağlar.

CVE Mapping

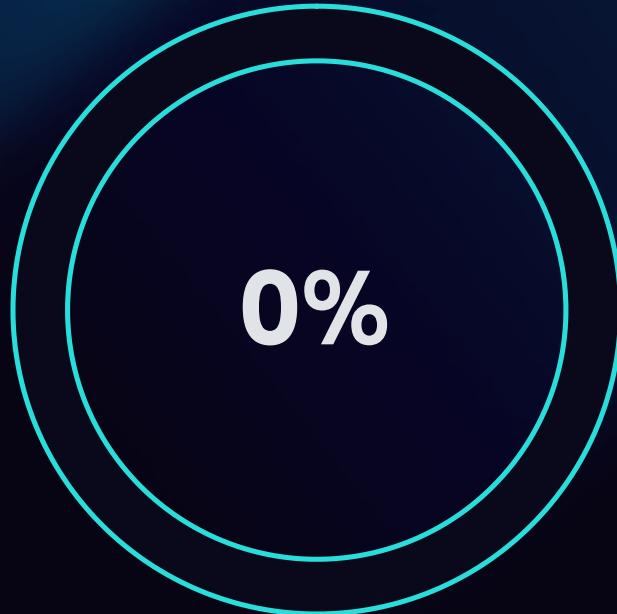
Hangi CVE'lerin hangi patch ile kapatıldığı açıkça görülür.

Güvenlik Metrikleri



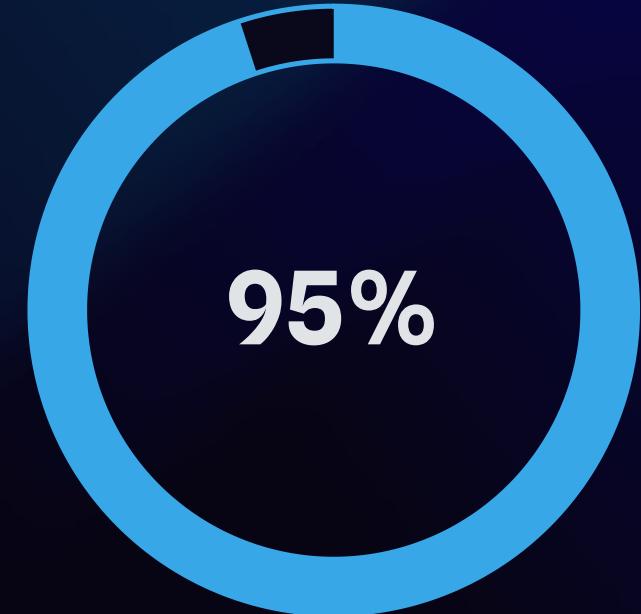
Otomasyon Oranı

Manuel işlem gereksinimi tamamen
elimine edildi



İnsan Hatası

Otomatik karar mekanizması ile hata
oranı sıfırlandı



Zaman Tasarrufu

Güvenlik güncellemeleri 20 kat daha
hızlı tamamlanıyor

SONUÇLAR

Proje Kazanımları



Zero Human Error

İnsan faktörü sistem güvenliğinden tamamen çıkarıldı. Kritik kararlar algoritma tarafından alınıyor.



Otomatik Patch Management

Güvenlik yamaları tespit anında uygulanıyor. Response time dakikalardan saniyelere düştü.



SecOps Compliance

Endüstri standartlarına uygun loglama ve audit trail sağlandı. Forensic analiz hazır.

LPMA

Gelecek Nesil Güvenlik

Autonomous Security

Sistem kendi güvenliğini yönetir

Real-Time Response

Tehditler anında neutralize edilir

Complete Visibility

Her işlem kayıt altında ve izlenebilir

[GITHUB.COM/LPMA-PROJECT](https://github.com/LPMA-PROJECT)

AHMET ARDA SEZER | 2026



Made with GAMMA